Volume 15, Issue 3

May 2014

The Computer Club At Willow Valley

Inside this issue:

The President's Pen by Sid Paskowitz

Membership As of this writing, your Computer Club has 517 paid members of the Club including 245 who have signed up as Lifetime members.

Thank You! First, I want to thank Dick Dressel and Ralph Beedle for their service as Computer Club Treasurer and Vice President respectively, and I want to thank Marge Schmieder who has volunteered to continue serving as Club Secretary. Welcome to Bob Scala, our new Vice President, and Charlie Trumbo, our new Treasurer. A reminder to Mac users, Bob Scala is a dyed-in-the-wool Mac user, so if you have suggestions or needs for programs at Computer Club meetings, which are Bob's responsibility for planning, let Bob know.

Mac SIG We are still looking for someone to lead the MAC SIG Group.

Recycling Ed Dahrsnin and his team are accepting working computers and components for recycling. Let Ed know if you would like to help recycle computers. Ed and his team meet on Monday afternoons at Manor North. Working in the recycling effort may also help you deal with your own computer when you have problems. Thanks to Ed and his team, the Computer Club recently passed the 100 mark of computer systems given to the Lampeter-Strasburg School District for families that cannot afford a computer.

(Continued on page 2)

The Apple Stand by JoAnne Phillips

Now that Macs and their associated devices have proliferated to the point where they are as attractive to the bad guys as a Windows machine used to be, it has become necessary for those of us fortunate enough to use this operating system to also emulate our Windows neighbors. We can no longer sit by, complacent because Macs don't get viruses. Today they do. Anyone operating a Mac believing they are safe is a foolish person just waiting to be attacked.

Good anti-virus and malware software is available for the download — and for free. I have used Bit Defender to clean up several machines lately and use it myself. I highly recommend it. You can download it here:

http://www.bitdefender.com/solutions/virus-scanner-for-mac.html •

Coming Programs

May 1, 2014
Sid Paskowitz, Resident
Windows 8

June 5, 2014
Ed Dahrsnin, Resident
Regular Cleaning Pays Off

July, 2014
No Meeting

All programs are held in the Theater at the Cultural Center on the 1st Thursday of the month at 2:00 p.m. unless otherwise noted.

President

(Continued from page 1)

Bylaws Updated At the April meeting the Computer Club, members voted to change the Club's bylaws to reflect a specific date on which newly elected officers would take office. The updated bylaws can be found on Information Central at http://resident.willowvalley.org/kiosk/cclub/p/bylaws.pdf or by clicking on the Bylaws link in Information Central.

Information Central For those of you who are not familiar with Information Central and the Computer Club Newsletter archive, you can access recent Newsletters and an index to topics in those Newsletters at http://resident.willowvalley.org/kiosk/cclub/p/Newsletter.pdf . The Newsletter index page is also available by left-clicking on Newsletter in the left column in Information Central.

Windows XP If you have a PC with the XP operating system installed, again be advised that as of April 8th 2014, Microsoft no longer supports XP or Office 2003. If your computer is not connected to the Internet and you do not expose it to risky external media such as thumb drives or hard drives, you shouldn't be concerned. However, if you have XP and connect to the Internet or external data sources, your computer can become increasingly at risk. The program at the May 1st Computer Club meeting will focus on updated Windows 8.1, the latest Microsoft operating system in case you are considering getting a new PC. Bring your questions. Come see what Windows 8.1 is all about.

Personal Protection Ok, now it is time for me to get on my soapbox again and repeat and re-emphasize information about personal computers and the Internet. I'm going to call it Personal Protection, because that is what it is! I don't care what kind of computer you have or what kind of protection your computer has, no computer can be 100% protected from malicious software. There are "bad guys" all over the world who spend their lives finding ways to infect your computer. Every time a company comes up with a way to help protect you, the "bad guys" look for ways to neutralize or get around those protections. Tony Poulos has put together a slide show that we display before Computer Club meetings. Watch the screen and learn how to protect yourself.

Zap2it At the April Computer Club meeting we showed a video tutorial about Zap2it, the online TV guide that displays the WVComTV (Willow Valley Communities TV) channel lineup. The video is available on the Computer Club's external Website at www.wvrccc.com. Be advised that the video was recorded prior to Tribune Media making a major change to Zap2it. As of the writing of this Presidents Pen, Zap2it is not taking new registrations; a six-hour option in lieu of a three hour display window is not available; and channel favorites (known as faves) cannot be identified and displayed at the top of the channel listings. On the other hand more selections such as movies or sports can be highlighted in the listing. I have received an email from Zap2it that they do plan to re-open registrations in

(Continued on page 3)

President

(Continued from page 2)

the near future and to restore the 6-hour display window option and favorites. Stay tuned. As stated in the tutorial video, expect changes and (hopefully) improvements.

Computer Club's External Website In case you hadn't noticed, below the number 2 at the top of the Information Central Home Page are links to the Computer Club External Website and to an index of topics covered in Information Central. Those links are highlighted to facilitate access to the powerful information sources.

Popups, popups Repeated reminders: If you get an unexpected pop-up, use Alt-F4 to clear it. If you click anywhere on the pop-up (and sometimes if you even put your cursor arrow on the pop-up), you could cause malicious software to run on your computer. There will be times when Alt-F4 will close a program you are running, but that may be better than infecting your computer.

If you get a popup advising you that an update is available such as for Firefox or Yahoo of Adobe or Java or Windows, or anything else, don't click on the popup. Use Alt-F4 to clear the popup, then go to the Website for that program by clicking on Help in that application or go to the company's Website and check for updates. The "bad guys" can create popups that look exactly like a legitimate notification; however, when you click on their popup, it takes you to their Website where your computer becomes infected.

Keep Up To Date Keep your software current, especially Adobe and Java, if you use them. Software companies try to fix the vulnerabilities in their software but they always lag the problem. Avoiding updates will subject you to risks from vulnerabilities that they have already fixed. It is bad enough that they always lag the problem, but you should not compound the problem by lagging it even further.

Stick To Simple If you only use your computer for basic email and you don't open unexpected emails and you don't click on popups, having Malwarebytes anti-malware and Microsoft Security Essentials or Windows Defender on your computer should be enough to give you basic protection. If you are a casual user, you probably don't need Java or other special software. The fewer the number of special applications, the fewer number of exploitable vulnerabilities the "bad guys" can take advantage of.

Kiosk Alternative I personally use a Resident Computer Kiosk unit to access my emails and do Internet searches. I also restart the Kiosk computer when I begin my session so it clears anything that someone using the computer before me may have done, and I restart the computer when I finish my session so someone using the computer after me cannot do anything to access what I have done. Even taking these actions, if you get a Kiosk unit infected during your session, the actions you take during your session will be at risk, but at least if you restart the computer after your session, the malware will be removed and later users will not be adversely affected by your actions.

(Continued on page 4)

A Cool Zoom Tip by Bob Wilcox

When you want to zoom in or out on a window, hold down CTRL and use the wheel on your mouse to zoom in and out. It works on the currently selected window. •

President

(Continued from page 3)

A Way to Verify Websites Whenever I am sent a link to a Website that I am not familiar with, I use www.siteadvisor.com to check out the site for malicious software before going to it. For example, someone suggested a "neat program" to me that I found was written by a company called sothinkmedia. I went to siteadvisor and entered that company's domain name and here is what siteadvisor displayed:

sothinkmedia.com

This link might be dangerous. We tested it and found security risks. Beware.

Website Category: Malicious Sites

Siteadvisor is a good tool that I use frequently when I browse the Web or want to check on a Website or company. Use a Kiosk unit to research new software before installing it. For example, I "Google" the product name and the words complaint or problem to see what others have written about that software. Games and music are notorious for infecting computers.

Unusual Email If you get an email that looks unusual or is in your Spam folder, don't open it on your computer. If you are really that curious about it, open it on a Resident Computer Kiosk unit. See what I said earlier about using a Resident Computer Kiosk unit.

Secret Guide to Computers and Tricky Living We have received notification from Russ Walter that his latest Secret Guide to Computers & Tricky Living 32nd Edition is now available. The regular price for the book or the book on CD is $25; however, based on past orders placed through the Computer Club, we are able to get the book or CD for $10 a copy. Anyone interested in ordering a copy, contact Charlie Trumbo at 464-6304. If you want to see some of what the book or CD contains, go to www.SecretFun.com.

Thank You My thanks to all of you who volunteer your time and knowledge to help other Residents. We need more volunteers! •

Heartbleed by Al Williams

You've heard about Heartbleed. You've heard that it is the worst security flaw ever for Internet users. But, what is it, how do you recognize it, and what should you do about it?

To protect user names, passwords, and data, encryption is frequently, but not always, used when moving information to or from your computer and a web site. You know that encryption is being used when you see https:// just before the web site's address in your browser. For example, https://www.awebsite.com indicates that this web site is using encryption.

For a long time this encryption was known as SSL (Secure Sockets Layer) but the name changed to TLS (Transport Layer Security) about 2 years ago as new capabilities were added. The new capabilities were implemented in three major software libraries: OpenSSL, GNU TLS, and Microsoft's Secure Channel. Unfortunately, the implementation of one new capability was not properly done in OpenSSL, but was done properly in the other two libraries.

(Continued on page 5)

Heartbleed

(Continued from page 4)

The flaw in the OpenSSL capability allows a knowledgeable person connected to a web site to obtain more information from the web site than they should. Instead of restricting access to just what was absolutely required, the flaw allows access to about 64,000 bytes of information. The knowledgeable person may repeat requests for information until all of the web site's server's memory has been read. A very clear visual of how this works may be found in comic format at xkcd.com/1354.

That requested information includes user names, passwords, user information, and the server's private encryption key. None of this is organized but a knowledgeable person can sort it and find the user names, passwords, information, and the key. It has been shown that this can be done with about 24 hours of effort but significantly most of the effort is automated so that no one must be present most of the time.

Is this a big problem? OpenSSL is a very popular software library and is used by many web sites; perhaps as many as 66% of all web sites. You do need to take steps to protect yourself.

Will the web sites notify their users of the problem? Although it is well known that accessing user information through the Heartbleed flaw does not leave any traces behind, some web sites are saying that they are not aware of any one accessing that data and are recommending that users continue with their current passwords. Their position is valid only if they had recorded ALL of the traffic to their web site for the past two years and reviewed every part of that traffic for Heartbleed information. If they have not recorded their traffic and reviewed it, they have no basis for saying that there are no problems.

How do I know if such and such web site is safe? This really is two questions: Was it safe at the time that the Heartbleed flaw was discovered? And, is it safe now? To determine if such and such web site is safe now, here are two web sites that will help: https://filippo.io/heartbleed/ and https://lastpass.com/heartbleed/ The lastpass site determines if the web site had been exploitable as well as its current status. If you are a LastPass user, it recommends actions to be taken.

I've heard that web sites are changing certificates in response to Heartbleed. Why? The certificate is linked to the site's private encryption key. When the site's private encryption key is captured using Heartbleed, all past and current communications with that web site may be read by the person holding that key. Once the key is changed, only past communications may be read but this is a significant amount of information.

To determine if the web site had not been safe, even though the above sites say that it is now, use the lastpass.com site above, or use the Perspectives add-on to the Firefox browser. The LastPass site will advise you if a password change is needed. For example, LastPass advises that all google.com passwords be changed unless you changed yours after Google fixed their site. This means that passwords on all Gmail accounts also need to be changed. Also, all Yahoo email account passwords and Twitter.com passwords need to be changed.

The Perspectives add-on provides dates for SSL certificates. If it shows that the SSL certificate for the web site that you are questioning changed after April 7, then you must assume owners of the web site determined that the certificate had to be changed meaning that the certificate was not safe prior to April 7 although it is now. In turn this means that you need to change your password.

(Continued on page 6)

Heartbleed

(Continued from page 5)

A solution to the problem of captured private encryption keys, either now or in the future, already exists. It is called forward secrecy and is sometimes called perfect forward secrecy. With forward secrecy, a permanent private encryption key based on the certificate is not used. Instead, an ephemeral key, a key that lasts for only a short time is used and is changed for each communication. A communication may be just part of a sentence. This means that an ephemeral key changes frequently and is typically valid for less than a minute. Why is this important? Because each communication, past or current, then has a unique encryption key and therefore each communication requires a separate effort to decrypt the communication. This becomes a formidable obstacle for anyone attempting to decrypt the communications.

A good way to determine if the web site is using forward secrecy is to use the Calomel add-on for Firefox. Clicking on the Calomel icon displays many security properties for that web site. One property is labeled perfect forward secrecy. A score of 20/20 or Yes is excellent. This is the minimum to be desired. To properly understand all of the properties being displayed, read the information at calomel.org. Look for the Firefox – "Calomel SSL Validation" link on the home page to access the add-on's explanation.

Is there more? Unfortunately, yes. OpenSSL is used in a variety of home electronics. For example, it is used by Cisco (Linksys) and Juniper in home routers which may make it possible to go through the router to your computer. Use Google with the term heartbleed and the name and model of your router to determine if your router is safe. Also, log into the administrative interface to your router and determine if the router's manufacturer has provided a firmware upgrade. If so, install the upgrade by carefully following the instructions. If you purchased your router before 2012, it is OK because the flaw was introduced into the OpenSSL library December 31, 2011 and was released for use by the public on March 14, 2012.

For most of us, the above describes the current extent of our exposure to Heartbleed. Hopefully this information will help you to understand the Heartbleed flaw, what to look for, and what to do about it. •

Would you like to read about a topic? Like to write about a topic?
Contact Sid Paskowitz or Al Williams

The Equipment Corner by Ed Dahrsnin

Refurbished Systems

#351: HP a1400e

#352: Dell 2400-4D7Y231

Miscellaneous We have 3 volt CR2023 batteries (suitable for motherboards to keep the system clock running) and a variety of CD-ROM's, floppy disk drives, keyboards, 2-button mice, various power supplies, and assorted cables. Please contact Ed Dahrsnin at 464-6591.

Donations We accept used, *working*, tower and laptop computers (with power units and batteries) from club members along with all software CDs. Used printer cartridges also accepted. You may deliver them to the North's Computer Resource room on the first floor of M building after 1 pm on Monday. No Macs or Mac parts, see JoAnne Phillips or Bob Handler for additional information. •

The Mission

The Mission of the Willow Valley Computer Club is to:

- Provide the means to educate beginners or interested non-users on how to use a computer.
- Arrange for speakers to talk to the Club about subjects that would be of interest to those with some background and experience in computer use.
- Provide a forum for interchange of computer information among members.

For more information about the Club, contact Sid Paskowitz at 464-2127 or wvcomputerclub@gmail.com •

The Leadership

Officers

President: Sid Paskowitz

Vice President: Bob Scala

Secretary: Marge Schmieder

Treasurer: Charlie Trumbo

Community Representatives

Manor: Larry Gallagher

Manor North: Lee Wermuth

Lakes: Gene Simasek

Committee Chairpersons

Program: Bob Scala

Training: Wayne Barner

Equipment: Ed Dahrsnin

Technical Support: Tony Poulos

Website: Sid Paskowitz

Publicity: Wally Gordon

Newsletter: Al Williams

Mac Interest Group:

Computer Room Coordinators:
Gene Simasek JoAnne Phillips

Microsoft Liaison: Ed Dahrsnin

Past Presidents

Larry Gallagher

Reviewer Acknowledgment

The following individual kindly reviewed this issue:

Sid Paskowitz

Thank you,

Al Williams

Interested in reviewing the Computer Club newsletter before it goes to press, providing advice about the content, or writing an article? Please contact:

Al Williams at atwilliams136@gmail.com